TikTok

June 30, 2022

The Honorable Marsha Blackburn
United States Senate
357 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Roger Wicker
United States Senate
555 Dirksen Senate Office Building
Washington, DC 20510

The Honorable John Thune
United States Senate
511 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Roy Blunt
United States Senate
260 Russell Senate Office Building
Washington, DC 20510

The Honorable Ted Cruz
United States Senate
127A Russell Senate Office Building
Washington, DC 20510

The Honorable Jerry Moran
United States Senate
521 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Shelley Moore Capito
United States Senate
172 Russell Senate Office Building
Washington, DC 20510

The Honorable Cynthia Lummis
United States Senate
124 Russell Senate Office Building
Washington, DC 20510

The Honorable Steve Daines
United States Senate
320 Hart Senate Office Building
Washington, DC 20510

Dear Senators Blackburn, Wicker, Thune, Blunt, Cruz, Moran, Capito, Lummis, and Daines,

Thank you for your letter dated June 27, 2022. We appreciate the opportunity to address the concerns you set forth. Many of your questions appear to stem from a recent BuzzFeed article, which contains allegations and insinuations that are incorrect and are not supported by facts. We appreciate the opportunity to set the record straight by answering your questions.

Before doing so, we would like to contextualize what many of the people quoted in the article were talking about and what the company has been broadly working to achieve. For well over a year, we've been pursuing a multi-pronged initiative called "Project Texas" to strengthen the company's data security program. Security experts can confirm that these initiatives are often painstaking and complex, even with expert assistance from world-class companies like Oracle and Booz Allen. Some people working on these projects do not have visibility into the full picture, working on a task

without realizing that it's a single step in a much bigger project or a test to validate an assumption.

That's critical context for the recordings leaked to Buzzfeed, and one thing their reporting got right: the meetings "*were in service of Project Texas's aim to halt this data access*."

The broad goal for Project Texas is to help build trust with users and key stakeholders by improving our systems and controls, but it is also to make substantive progress toward compliance with a final agreement with the U.S. Government that will fully safeguard user data and U.S. national security interests. We have not spoken publicly about these plans out of respect for the confidentiality of the engagement with the U.S. Government, but circumstances now require that we share some of that information publicly to clear up the errors and misconceptions in the article and some ongoing concerns related to other aspects of our business.

While we are disappointed that leaks have put us in this position, we are pleased to share the substantial progress on our objectives. As we recently reported, we now store 100% of U.S. user data by default in the Oracle cloud environment, and we are working with Oracle on new, advanced data security controls that we hope to finalize in the near future. That work puts us closer to the day when we will be able to pivot toward a novel and industry-leading system for protecting the data of our users in the United States, with robust, independent oversight to ensure compliance.

We are taking additional measures beyond data security, which we will briefly touch on in our responses below.

We have been clear dating back to an early 2020 blog post that we are working on a broad set of objectives: "*Similar to industry peers, we will continue to drive our goal of limiting the number of employees who have access to user data and the scenarios where data access is enabled. Although we already have controls in place to protect user data, we will continue to focus on adding new technologies and programs focused on global data residency, data movement, and data storage access protections worldwide*." (https://newsroom.tiktok.com/en-us/our-approach-to-security). There is a distinction between data storage and data access, but they are both—together—important components of our efforts to earn trust and improve security for TikTok; our solution will now ensure both the storage of all U.S. user data in the United States and all data sharing outside of the protected enclave in the United States will be pursuant to protocols and terms approved by the U.S. Government.

In light of the context above, we are confident that when you review our responses, you will see that TikTok has not, at any point, misled Congress about our data and security controls and practices. We understand, respect, and appreciate the incredibly important work of your Committee and Congress, and we have always approached our engagements with Members and staff, both in public and in private, with candor and

integrity. We stand by the statements Michael Beckerman made before Congress and are grateful for his leadership.

As we continue our productive conversations with the Administration and continue to explore commercial partnerships with companies like Oracle, we look forward to keeping you and the full Committee apprised of our work to further ensure the security of U.S. user data.

Please see below for TikTok's responses to your questions.

1. **Is it true that TikTok employees located in China currently have, or had in the past, access to U.S. user data? This could include programmers, product developers, data teams, as well as trust and safety and content moderation professionals.**
    a. **If yes, please explain in detail which employees have or had such access and for what purposes.**
    b. **If the employees had this access in the past but no longer do, please identify the applicable date ranges.**

Employees outside the U.S., including China-based employees, can have access to TikTok U.S. user data subject to a series of robust cybersecurity controls and authorization approval protocols overseen by our U.S.-based security team. In addition, TikTok has an internal data classification system and approval process in place that assigns levels of access based on the data's classification and requires approvals for access to U.S. user data. The level of approval required is based on the sensitivity of the data according to the classification system.

The solution that TikTok is implementing pursuant to Project Texas has focused on evaluating and revising TikTok's internal policies and operational controls in relation to U.S. user data access, to take steps to strengthen data security around U.S. user data and, ultimately, to make the organizational, process, and technical changes to help ensure compliance and enhance protection of U.S. user data defined as "protected" through engagement with CFIUS. As we are in the process of undergoing CFIUS national security review, we have kept CFIUS informed of these efforts. This protected user data will be stored in Oracle Cloud Infrastructure with access limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government.

2. **TikTok's privacy policy says you share data you collect with your parent companies and affiliates and that you transmit user information to servers and data centers overseas.**
    a. **Have any ByteDance employees—located in China or elsewhere—had access to U.S. User data, either currently or in the past?**

Please see our response to question 1.

b. What are the locations of the servers and data centers overseas where TikTok transmits U.S. user data?

TikTok has long stored U.S. user data in data centers in the U.S. and Singapore, as well as in cloud-based services offered by AWS, the Google Cloud Platform, and Azure. Our Virginia data center includes physical and logical safety controls such as gated entry points, firewalls, and intrusion detection technologies. It is also important to maintain backup data storage locations to guard against catastrophic scenarios where user data could be lost, and our data center in Singapore serves as the backup data storage location for our U.S. user data.

100% of U.S. user traffic is now being routed to Oracle Cloud Infrastructure. We are still using our U.S. and Singapore data centers for backup, but as we continue our work to deliver on U.S. data governance, we expect to delete U.S. users' protected data from our own systems and fully pivot to Oracle cloud servers located in the U.S.

3. Do any ByteDance employees have a role in shaping TikTok's algorithm?

Subject to the controls described in our response to question 1, ByteDance engineers around the world may assist in developing those algorithms, however our solution with Oracle will ensure that training of the TikTok algorithm only occurs in the Oracle Cloud Infrastructure and will also ensure appropriate third-party security vetting and validation of the algorithm. For more information about how TikTok's algorithm recommends content, please see our Newsroom post: https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you.

4. Do any Douyin employees have any access to American user data or a role in shaping TikTok's algorithm?

ByteDance developed the algorithms for both Douyin and TikTok, and therefore some of the same underlying basic technology building blocks are utilized by both products, but TikTok's business logic, algorithm, integration, and deployment of systems is specific to the TikTok application and separate from Douyin.

Under Project Texas and as a result of our work with the U.S. Government, going forward our solution with Oracle will ensure the TikTok application and platform, including the algorithm, is deployed through the Oracle Cloud Infrastructure in the United States with third-party security vetting and validation of the software for the application and platform, including the TikTok algorithm.

5. **In the past, TikTok has said that it has never—nor would it ever—provide user data to the Chinese government, even if asked. Yet your privacy policy says you can disclose data collected to respond to government inquiries.**
    a. **Has TikTok ever disclosed any U.S. user data to respond to government inquiries from the Chinese Communist Party?**
    b. **If the Chinese Communist Party asked you for U.S. user data, what is to stop you from providing it? Can the CCP compel you to provide this data, regardless of response? Can they access it, regardless of response?**
    c. **Has ByteDance ever responded to CCP inquiries on TikTok's behalf?**
    d. **Has TikTok ever shared U.S. user data with ByteDance for the purpose of responding to a CCP inquiry?**

We have not been asked for such data from the CCP. We have not provided U.S. user data to the CCP, nor would we if asked.

More information about government requests for user data that we receive across the world is available in our Information Request Reports, available at https://www.tiktok.com/transparency/en-us/information-requests-2021-1/.

6. **Do TikTok employees in the U.S. use software developed by ByteDance, such as Lark?**

Yes.

7. **Does ByteDance have any role—either in the past or in the present—in hiring TikTok employees in the U.S.?**

As would be expected of any global company with subsidiaries, ByteDance plays a role in the hiring of key personnel at TikTok. However, as we have described before, TikTok is led by its own global CEO, Shou Zi Chew, a Singaporean based in Singapore.

8. **Does TikTok own or lease its own office space in the U.S., and does ByteDance have any ownership or lease stake in those facilities?**

TikTok leases office space in cities across the U.S., including Los Angeles, Austin, Chicago, New York, Detroit, Seattle, DC, and Nashville. These leases are through U.S. entities, TikTok Inc. (a California corporation) and ByteDance Inc. (a Delaware corporation).

9. **Does the Chinese government have an ownership stake or seat on the Board of Directors, or provide personnel in any other leadership position, of the Beijing ByteDance Technology Company?**

a. **What role does this seat play in impacting decisions made at ByteDance or TikTok?**
b. **Does this position afford an opportunity for the board member to determine whether and how TikTok or ByteDance will respond to CCP inquiries?**
c. **Does this position afford an opportunity for the board member to view TikTok user data?**
d. **Would you be informed, as a matter of policy, if a board member did view the data? If the board member did share the data, in any capacity, with the CCP?**

As multiple corporate entities share the "ByteDance" name, several China-based ByteDance entities were renamed earlier this year to keep the names of businesses and entities more consistent. Beijing Bytedance Technology Co. Ltd is now called Beijing Douyin Information Service Limited. We will refer to it here using its new name for avoidance of confusion.

ByteDance Ltd., the ultimate parent entity that is incorporated in the Cayman Islands, has a global board, including Bill Ford of General Atlantic, Arthur Dantchik of Susquehanna International Group, Philippe Laffont of Coatue, Neil Shen of Sequoia, and the company's CEO Rubo Liang. The majority of ByteDance's investors are global institutional funds such as Coatue, General Atlantic, KKR, Sequoia, Softbank, and Susquehanna International Group.

Beijing Douyin Information Service Limited is a separately held subsidiary of ByteDance Ltd. Beijing Douyin Information Service Limited does not have any direct or indirect ownership interest in or control over any TikTok entity. Further, employees of Beijing Douyin Information Service Limited are restricted from U.S. user database access. The Chinese state-owned enterprise's acquisition of 1% of Beijing Douyin Information Service Limited was necessary for the purpose of obtaining a news license in China for several China-based content applications, such as Douyin and Toutiao.

The Chinese government does not directly or indirectly have the right to appoint board members or otherwise have specific rights with respect to any ByteDance entity within the chain of ownership or control over the TikTok entity.

10. **How will TikTok's new cloud service arrangement be structured, and how will the company determine which data is "protected" such that it is not shared with employees or others in China?**

TikTok recently published a Newsroom post outlining our U.S. data governance practices and announcing a commercial relationship with Oracle in support of these practices (https://newsroom.tiktok.com/en-us/delivering-on-our-us-data-governance).

As described in question 1, U.S. user data at issue is being defined as “protected” through engagement with CFIUS, and will be stored in the Oracle Cloud Infrastructure with access limited only to certain personnel in USDS. Under the contemplated arrangement, access to U.S. user data by anyone outside of USDS will be limited by, and subject to, robust data access protocols, with further monitoring and oversight mechanisms by Oracle to validate compliance.

In order to facilitate a global platform, non U.S.-based employees, including China-based employees, will have access to a narrow set of non-sensitive TikTok U.S. user data, such as public videos and comments available to anyone anywhere in the world, to ensure global interoperability so our U.S. users, creators, brands, and merchants are afforded the same rich and safe TikTok experience as global users.

11. Why is TikTok not planning to ensure that all U.S. user data is blocked from view of employees or others in China?

As described in our response to question 10, access to U.S. user data by anyone outside of our new USDS team will be limited by, and subject to, robust data access protocol that will be developed in close collaboration with Oracle and CFIUS.

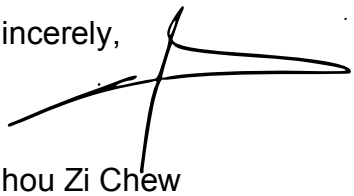
We’re proud to be able to serve a global community of more than a billion people who use TikTok to creatively express themselves and be entertained, and we’re dedicated to giving them a platform that builds opportunity and fosters connections worldwide. We also work hard to safeguard our community, both in how we address potentially harmful content and how we protect against unauthorized access to user data.

Consistent with the operation of this global platform, and as described in our response to question 10, certain China-based employees will have access to a narrow, non-sensitive set of TikTok U.S. user data, such as the public videos and comments available to anyone, to ensure global interoperability so our U.S. users, creators, brands, and merchants are afforded the same rich and safe TikTok experience as global users. But this access will be very limited, it will not include private TikTok U.S. user information, and it will only occur pursuant to protocols being developed with the U.S. Government.

*****

We thank you for your questions and appreciate the opportunity to provide additional details and clarification. We know we are among the most scrutinized platforms from a security standpoint, and we aim to remove any doubt about the security of U.S. user data. We're dedicated to earning and maintaining the trust of our community and of policymakers, and will continue to work every day to protect our platform and provide a safe, welcoming, and enjoyable experience for our community.

Sincerely,



Shou Zi Chew
CEO, TikTok

cc:
The Honorable Maria Cantwell
The Honorable Richard Blumenthal